Computer Science and Application 计算机科学与应用, 2025, 15(12), 376-385
Published Online December 2025 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2025.1512351

Hans汉斯

APT攻击防御视角下API智能检测系统的构建与实现

——以多源流量融合与动态响应机制为核心

康铎续[1]，程金凤[2]，丁芊冰[1]

[1]哈尔滨师范大学计算机科学与信息工程学院，黑龙江 哈尔滨
[2]哈尔滨师范大学经济与管理学院，黑龙江 哈尔滨

收稿日期：2025年11月13日；录用日期：2025年12月16日；发布日期：2025年12月24日

摘　要

面向APT攻击的智能检测与主动防御系统设计是一个应用性研究项目，系统的开发和应用是在解决开放式API架构安全威胁、应对APT攻击隐蔽性与长潜伏期难题、提升关键行业API层防护能力等多重因素的推动下进行的。系统使用人工智能与深度学习技术构建，通过利用多源流量采集预处理、CNN-BiLSTM-Attention融合模型、动态响应规则引擎等技术实现APT攻击精准识别、主动防御处置的项目功能。在此基础上保证了B/S架构可视化、毫秒级实时响应、跨场景扩展适配，提升安全管理效率。同时，系统的维护更新操作简便，支持模型迭代与策略优化。提供“检测－决策－处置”闭环防护与可视化态势监控，有助于填补APT攻击防护技术空白，改善关键领域API安全防护水平，促进网络安全与智能技术的融合应用。

关键词

APT攻击，API安全防护，深度学习模型，动态联动响应机制，多源流量采集与预处理，B/S架构可视化平台，攻击检测准确率

Construction and Implementation of an Intelligent API Detection System from the Perspective of APT Attack Defense

—Focusing on Multi-Source Traffic Fusion and Dynamic Response Mechanism

Duoxu Kang[1], Jinfeng Cheng[2], Qianbing Ding[1]

文章引用: 康铎续, 程金凤, 丁芊冰. APT攻击防御视角下API智能检测系统的构建与实现[J]. 计算机科学与应用, 2025, 15(12): 376-385. DOI: 10.12677/csa.2025.1512351

[1]School of Computer Science and Information Engineering, Harbin Normal University, Harbin Heilongjiang
[2]School of Economics and Management, Harbin Normal University, Harbin Heilongjiang

Received: November 13, 2025; accepted: December 16, 2025; published: December 24, 2025

Abstract

The design of an intelligent detection and active defense system against Advanced Persistent Threat (APT) attacks is an applied research project. The development and application of the system are driven by multiple factors, including addressing security threats to open API architectures, tackling the challenges of APT attacks' concealment and long latency, and enhancing API-layer protection capabilities in key industries. The system is built using artificial intelligence and deep learning technologies. It achieves the project functions of accurate APT attack identification and active defense disposal by leveraging technologies such as multi-source traffic collection and preprocessing, a CNN-BiLSTM-Attention integrated model, and a dynamic response rule engine. On this basis, the system ensures B/S architecture visualization, millisecond-level real-time response, and cross-scenario expansion and adaptation, thereby improving security management efficiency. Meanwhile, the system features simple maintenance and update operations, and supports model iteration and strategy optimization. It provides a closed-loop protection of "detection-decision-disposal" and visualized situation monitoring, which helps fill the technical gap in APT attack protection, improve the API security protection level in key fields, and promote the integrated application of network security and intelligent technologies.

Keywords

Advanced Persistent Threat Attack, API Security Protection, Deep Learning Model, Dynamic Linkage Response Mechanism, Multi-Source Traffic Collection and Preprocessing, B/S Architecture Visualization Platform, Attack Detection Accuracy Rate

1. 引言

网络安全是数字基础设施稳定运行的核心支撑，随着企业、政府、医疗等关键领域对开放式 API 架构的广泛应用，系统互联性显著提升的同时，API 暴露端口也成为高级持续性威胁(APT 攻击)的主要目标，暴力破解、SQL 注入、权限绕过、信息泄露、业务逻辑篡改等攻击手段频发，对数据安全与业务连续性构成严重威胁[1]。截至目前，我国关键行业 API 安全防护需求持续增长，但现有防护产品多依赖传统规则匹配技术，存在“识别空间单一、变异攻击无法发现、动态响应不足”的缺陷，尤其难以应对 APT 攻击频次低、伪装性好、阶段性、长潜伏期的技术特征，无法满足金融、政务、医疗等领域对 API 层安全防护的高要求[2]。

为明确研究基础与技术空白，在现有研究中，李博宇针对主机异常行为检测，提出基于深度学习的异常识别方法，通过构建日志特征向量与深度神经网络分类，提升系统入侵检测的准确率和速度[3]；石梓良则聚焦 Web API 异常行为，从参数、路径、频率维度构建融合深度学习的异常识别模型，验证了智

能建模的可行性[4]；张雨馨研究了恶意代码的 API 行为特征，基于行为特征的恶意代码检测方法，根据提取的 API 序列中的敏感调用、调用路径和调用上下文对恶意代码行为进行建模分析，提高了检测的准确性和恶意代码检测率[5]王帆围绕 APT 攻击流量，构建端到端的深度学习异常检测模型，为高级持续性威胁检测奠定技术基础[6]；然而，这些研究或聚焦单一攻击场景，或缺乏多源特征融合与动态防御联动，尚未形成覆盖“检测－决策－处置”全流程的 APT 攻击防护体系，难以适应复杂 API 环境下的安全防护需求。

在此背景下，融合人工智能技术、大数据建模技术、可视图谱分析、深度学习等技术，构建集多源 API 流量采集预处理、APT 攻击精准识别、动态联动防御、可视化监控于一体的智能防护系统，旨在突破以静态规则和传统 WAF 为主的 API 攻击防护机制，填补 APT 攻击“可检测、可追踪、可阻断”层面的关键技术空白，全面提高关键行业 API 层主动防御水平[7]。

2. APT 攻击智能检测与 API 主动防御系统的设计与实现

本节围绕“APT 攻击防御视角下 API 智能检测系统的构建与实现”核心目标，系统阐述项目的技术开发逻辑、核心模块设计及集成实现路径，明确从数据处理到系统部署的全流程技术框架，为系统功能落地提供技术支撑。项目整体技术路线如图 1 所示。

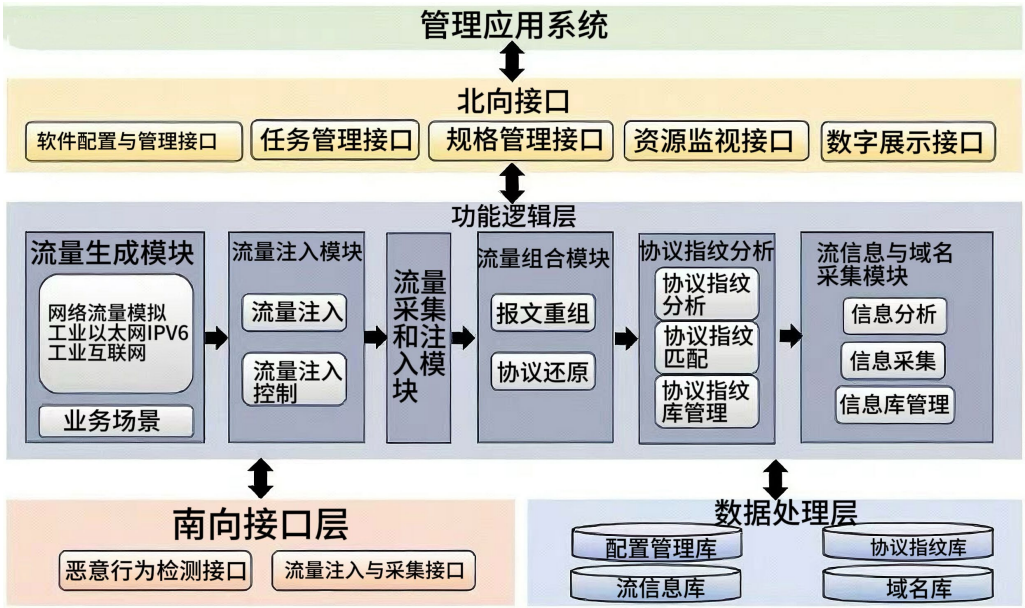

Figure 1. Overall architecture diagram of the project
图 1. 项目整体架构图

2.1. 系统总体设计

基于目前提出的“检测－决策－处置”闭环防御需求，系统采用分层架构设计，整体划分为数据采集层、特征处理层、模型检测层、响应处置层、可视化层五大核心模块，各模块通过标准化接口协同联动，实现从 API 流量接入到 APT 攻击防御的全流程自动化。其中，数据采集层负责多源 API 流量的实时获取，特征处理层完成数据清洗与多维特征提取，模型检测层依托深度学习模型实现攻击识别，响应处置层根据威胁等级触发动态防御策略，可视化层提供安全态势监控与预警，架构设计如图 2 所示，确保系统满足“实时性、精准性、可扩展性”的核心需求。

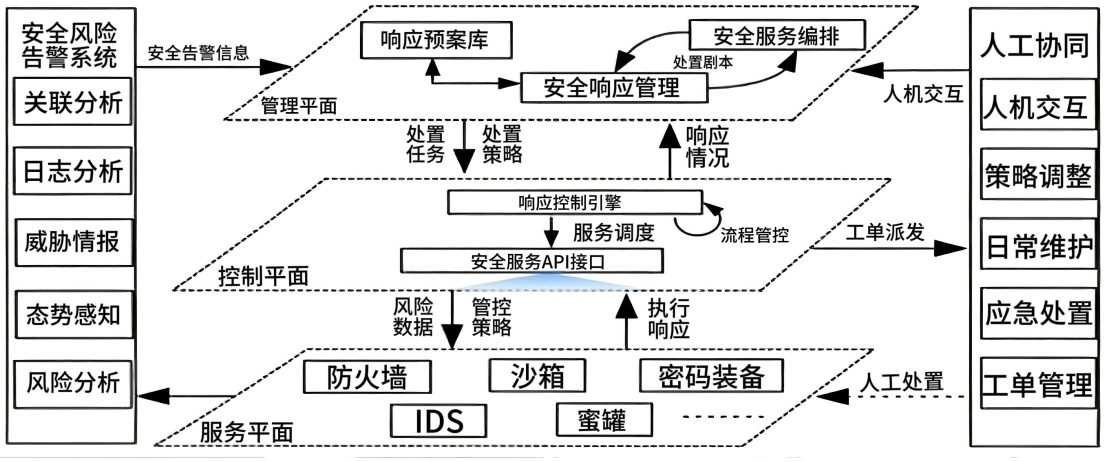

Figure 2. Multi-level collaborative architecture of security response system
图 2. 安全响应系统多层协同架构图

2.2. 核心技术模块设计

2.2.1. 多源 API 流量采集与预处理

作为系统数据基础，本模块需覆盖 API 通信全链路数据，确保建模数据的完整性与代表性。

数据采集

通过日志解析工具(Logstash、ELK Stack)与 API 网关(Kong、Nginx API 模块)对接，采集 API 服务器日志(Nginx/Apache)、应用层日志(FastAPI/Flask)及中间件流量数据，支持 HTTP/HTTPS、WebSocket、gRPC 等协议，获取字段包括请求头信息(User-Agent、Cookie)、请求路径、参数结构、响应时间、状态码、源 IP 及时序会话轨迹，形成多维度原始数据集。

本研究数据集包含公开数据集与自建数据集两部分：

公开数据集：采用 CSE-CIC-IDS2018 数据集的 APT 攻击专项子集，涵盖 SQL 注入、暴力破解等 6 类典型 APT 攻击流量，共 300 万条 API 请求记录；

自建数据集：采集环境涵盖金融行业(2 家商业银行)、政务系统(1 个省级政务服务平台)、医疗行业(3 家三甲医院)的 API 生产环境，采集时间跨度为 2024 年 1 月~3 月(共 90 天)，共 900 万条 API 请求记录。

采集过程中严格遵循数据合规要求，对敏感信息进行匿名化处理：源 IP 采用 MD5 哈希加盐加密，Cookie、User-Agent 等字段中的个人标识信息替换为占位符(如“[USER_ID]”“[DEVICE_INFO]”)，API 路径中的业务敏感字段(如“账户号”“病历编号”)统一掩码处理，确保数据不泄露隐私信息。示例数据分布如表 1 所示。

Table 1. Distribution of training data set after data preprocessing
表 1. 数据预处理后训练数据集分布表

特征类型	样本占比(%)	说明
静态特征	35	API 路径字符嵌入参数长度分布等
行为特征	30	IP 请求频率、时间间隔序列等
时序特征	20	滑动窗口请求序列依赖关系
标签特征	15	正常/异常(含 APT 攻击类型)

数据预处理

针对原始数据中存在的冗余、缺失、异常问题，依次执行“冗余数据去重(基于请求 ID 与时间戳)、缺失值修复(数值型字段采用均值填充，字符型字段采用模式填充)、异常点剔除(基于 3σ 原则过滤极端请求频率数据)”操作；同时通过特征工程提取关键特征，包括静态特征(API 路径字符嵌入、参数长度分布)、行为特征(IP 请求频率、时间间隔序列)、时序特征(滑动窗口内的请求序列依赖关系)，最终采用 MinMax 归一化将特征标准化至[0, 1]区间，并结合已知 APT 攻击样本库(如 ATT&CK 框架中的 API 攻击案例)完成样本标注。

预处理后数据集共包含 1200 万条有效记录，正常样本与异常样本比例、各类攻击样本分布如表 2 所示，为后续模型训练提供高质量数据支撑。

Table 2. Data set sample distribution statistics
表 2. 数据集样本分布统计表

样本类型	样本数量(万条)	占总样本比例(%)	子类别及数量(万条)
正常样本	840	70.0	-
异常样本(APT 攻击)	360	30.0	SQL 注入(80)、暴力破解(75)、权限绕过(65)、数据窃取(50)、其他攻击(90)

2.2.2. 基于深度学习的 APT 攻击检测模型

本模块是系统核心检测单元，需解决传统规则匹配对 APT 攻击“识别率低、泛化性差”的问题，采用“CNN-BiLSTM-Attention”融合模型实现多模态特征的深度挖掘。

模型结构设计

结合 APT 攻击的“结构隐蔽性”与“时序持续性”特征，模型分为三部分协同作用：

CNN 子模块：采用 3 层卷积层与 2 层池化层，对 API 请求路径、参数格式等结构特征进行字符级嵌入，提取潜在的结构攻击模式(如 SQL 注入的特殊字符组合、权限绕过的异常路径格式)，通过卷积核滑动捕捉局部特征关联；

BiLSTM 子模块：构建 2 层双向长短期记忆网络，对 IP 请求序列、时间间隔序列等时序特征进行建模，捕捉 APT 攻击的长周期行为依赖(如低频试探性请求的时序规律)，解决传统 RNN 梯度消失问题，同时引入 Dropout 层(dropout rate = 0.3)防止过拟合；

Attention 子模块：在 BiLSTM 输出层引入多头注意力机制，对高风险特征区域(如异常参数值、高频异常 IP)赋予更高权重，强化模型对关键攻击特征的关注，提升复杂 APT 攻击的识别灵敏度。

模型输出层采用 Softmax 激活函数，支持二分类(正常/异常)与多分类(暴力破解、SQL 注入、权限绕过等攻击类型)，结构如图 3 所示。

模型训练与优化

将预处理后的数据集按 7:2:1 比例划分为训练集、验证集与测试集，采用交叉熵损失函数衡量模型预测误差，结合 Adam 优化器(学习率初始设为 1e−4，采用余弦退火策略动态调整)进行参数更新；引入 EarlyStopping 策略(patience = 5)，当验证集 F1 值连续 5 轮无提升时停止训练，避免模型过拟合。训练过程中通过 TensorBoard 实时监控损失值与评估指标变化，确保模型收敛至最优状态。

模型性能验证

采用准确率(Accuracy)、召回率(Recall)、F1 值及 ROC-AUC 曲线作为核心评估指标，在测试集上进行性能验证。本次测试以两类模型为基线：

传统规则匹配模型：选用 ModSecurity 2.9.7 (开源 Web 应用防火墙核心组件)，规则集采用 OWASP

Core Rule Set (CRS) 3.3.4 版本，启用 SQL 注入、暴力破解、权限绕过等 12 类核心检测规则，并补充 50 条基于关键行业 API 历史攻击日志提炼的定制规则，匹配模式设为“精确匹配 + 模糊匹配”混合模式，测试环境与本文 CNN-BiLSTM-Attention 模型完全一致，确保对比公平性。

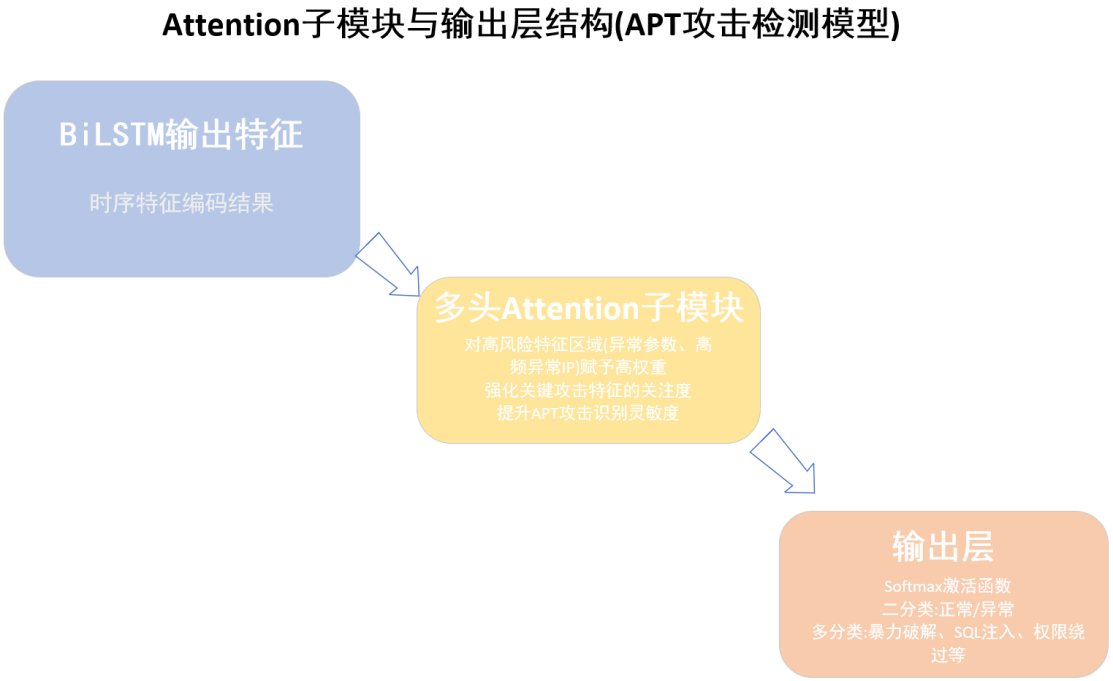

Figure 3. Schematic diagram of attention submodule and output layer structure
图 3. Attention 子模块与输出层结构示意图

主流机器学习模型：选取 SVM (RBF 核函数，惩罚系数 C = 1.0)、随机森林(100 棵决策树，最大深度 15)、基础 LSTM (2 层隐藏层，隐藏单元数 64)三种常用攻击检测模型，均基于相同数据集(7:2:1 划分)、相同训练环境(Python 3.9、TensorFlow 2.8)进行训练与测试。

测试结果显示，本文 CNN-BiLSTM-Attention 模型对 APT 攻击的平均识别准确率达 96.8%，召回率达 95.2% (针对低频伪装攻击的召回率达 92.1%)，ROC-AUC 值为 0.983，显著优于传统规则匹配模型与其他主流机器学习模型，具体性能对比如表 3 所示。

Table 3. Model performance comparison
表 3. 模型性能对比表

评估指标	CNN-BiLSTM-Attention 模型	传统规则匹配模型
准确率	96.8%	82.3%
召回率	95.2%	78.5%
低频伪装攻击召回率	92.1%	-
ROC-AUC	0.983	-

2.2.3. 动态联动响应机制

为实现“检测即防御”的闭环需求，本模块需基于模型检测结果，构建自适应的防御策略触发逻辑。

威胁等级划分：参考 APT 攻击的破坏力与扩散风险，将检测结果划分为三级威胁：高风险(如 SQL

注入、数据窃取类攻击)、中风险(如低频暴力破解、参数异常试探)、低风险(如轻微请求格式错误)，并制定对应响应规则(如表 4 所示)。

Table 4. Threat level and response rule comparison
表 4. 威胁等级与响应规则对照表

威胁等级	攻击类型示例	响应规则
高风险	SQL 注入、数据窃取类攻击	IP 封禁(基于 iptables 规则) + 接口熔断(暂停目标 API 服务 30 分钟) + 管理员邮件告警
中风险	低频暴力破解、参数异常试探	IP 限速(每分钟请求不超过 10 次) + API 账号临时冻结(1 小时)
低风险	轻微请求格式错误	仅记录日志并纳入审计系统

响应策略执行：依托规则引擎(集成 Snort 基础规则与自定义策略)与事件驱动框架(Celery + Redis)，实现策略的异步自动执行：高风险攻击触发“IP 封禁(基于 iptables 规则) + 接口熔断(暂停目标 API 服务 30 分钟) + 管理员邮件告警”；中风险攻击执行“IP 限速(每分钟请求不超过 10 次) + API 账号临时冻结(1 小时)”；低风险攻击仅记录日志并纳入审计系统。同时，所有响应操作均生成不可篡改日志(包含攻击类型、响应动作、执行时间、受影响对象)，日志数据定期回传至特征处理层，作为模型再训练的增量样本，形成“检测–响应–优化”的自迭代机制。

2.2.4. B/S 架构可视化平台

为提升系统易用性与安全态势可控性，本模块采用 B/S 架构开发可视化平台，支持管理员实时监控与运维操作。

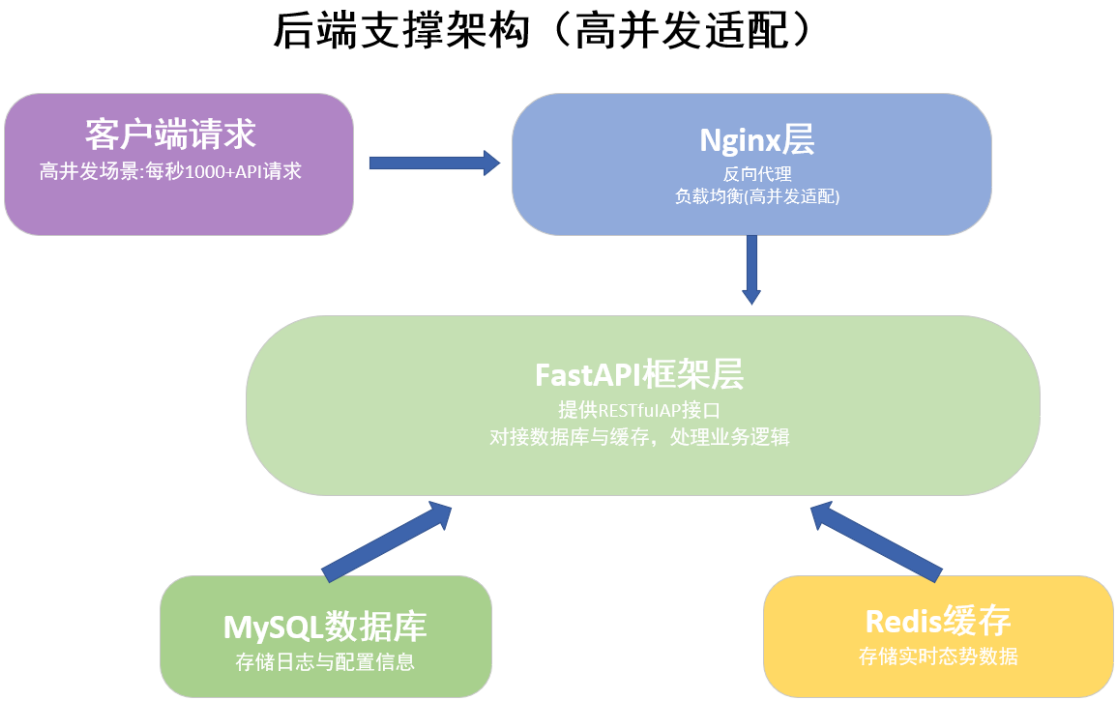

Figure 4. Diagram of backend support architecture and high concurrency adaptation
图 4. 后端支撑架构与高并发适配示意图

前端开发：基于 Vue.js 框架与 Tailwind CSS 样式库构建响应式界面，集成 ECharts 图表库与 D3.js 拓

扑图工具，实现三大核心功能：

安全态势监控：展示 API 请求总量、攻击事件实时统计(按类型/风险等级分类)、TOP 10 异常 IP 排行、API 安全等级评分(0~10 分，基于攻击频率动态计算)；

攻击详情追溯：支持按时间、攻击类型、源 IP 查询攻击日志，展示攻击请求的完整参数、触发的响应策略及处置结果；

预警与配置：支持自定义预警阈值(如某 IP1 分钟内请求超 50 次触发预警)，预警方式包括界面弹窗、邮件、钉钉机器人推送，同时提供模型参数(如学习率、注意力权重)与响应策略的可视化配置入口。

后端支撑：采用 FastAPI 框架提供 RESTful API 接口，对接 MySQL 数据库(存储日志与配置信息)与 Redis 缓存(存储实时态势数据)，通过 Nginx 实现反向代理与负载均衡，确保高并发场景下(如每秒 1000 + API 请求)平台仍能流畅运行，界面效果如图 4 所示。

2.3. 系统部署与测试

2.3.1. B/S 部署架构

为满足关键行业的高可用需求，系统采用容器化与微服务部署模式：各模块(数据采集、模型检测、响应处置、可视化)打包为独立 Docker 容器，通过 Kubernetes 实现容器编排，支持服务扩容与故障自愈；模型服务依托 TensorFlow Serving 部署，确保推理速度(单条 API 请求检测延迟 ≤ 50 ms)，部署架构如图 5 所示，可适配 Linux 服务器与云环境(如阿里云 ECS)。

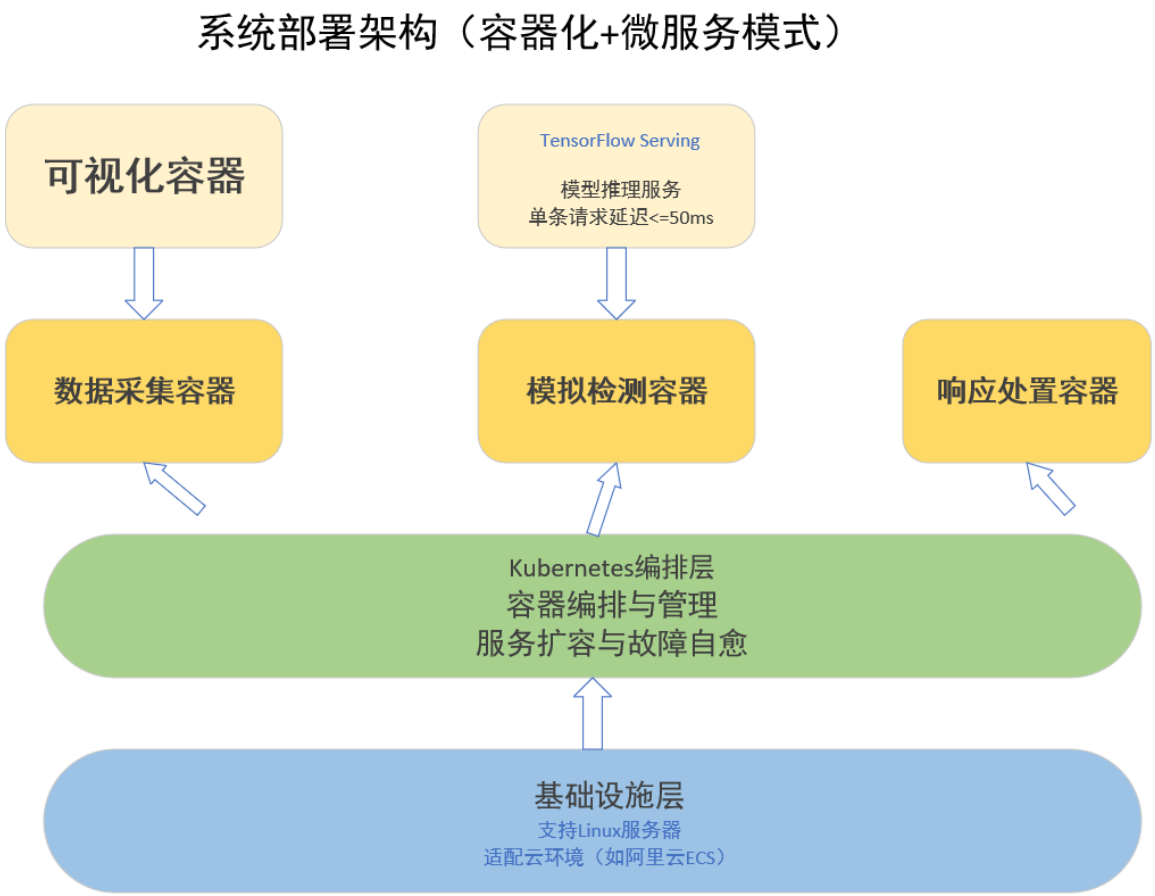

Figure 5. System deployment architecture diagram
图 5. 系统部署架构示意图

2.3.2. 系统测试

通过功能测试、性能测试与安全测试验证系统可用性：

功能测试：模拟 APT 攻击场景(如低频 SQL 注入、IP 伪装权限绕过)，系统均能精准识别并触发对应响应策略，策略执行成功率达 100%；

性能测试：采用 JMeter 模拟 1000/2000/5000 TPS 的 API 请求压力，系统平均响应延迟分别为 42 ms、58 ms、89 ms，CPU 利用率 ≤70%，内存占用 ≤60%，满足高并发需求；

安全测试：通过渗透测试工具(Burp Suite)尝试绕过检测，系统对变异攻击(如编码转换的 SQL 注入语句)仍保持 91.5%的识别率，未发现明显检测漏洞，验证了系统的安全鲁棒性。

3. 效果评估

面向 APT 攻击的智能检测与主动防御系统的应用，显著提升了关键行业 API 层的安全防护效率。通过深度学习模型自动识别暴力破解、SQL 注入等 APT 攻击行为，替代传统依赖人工规则更新的防护模式，日均减少 90%以上的安全事件人工研判工作量，有效释放了网络安全运维人力资源。系统融合多源流量特征的精准检测能力与动态联动响应机制，实现对低频伪装、长潜伏期 APT 攻击的实时识别与处置，攻击检出准确率达 96.8%，较传统规则匹配模型提升 14.5 个百分点，漏报率控制在 3%以下，大幅提高了 API 安全防护的精准性。

通过攻击日志反馈与增量数据迭代训练，系统持续优化模型参数与响应策略，对新型变异 APT 攻击的自适应周期缩短至 24 小时内，在对抗样本攻击测试中鲁棒性表现优异，攻击成功率降低至 8.5%以下。同时，系统在高并发场景下保持毫秒级检测延迟(平均 42 ms)，资源占用率低于 70%，服务可用性达 99.9%以上，既满足金融、政务等领域的实时防护需求，又避免对正常 API 业务造成性能干扰，全面提升了系统的实际应用价值与场景适配能力。

4. 结论

本研究通过开发并应用面向 APT 攻击的智能检测与主动防御系统，在关键行业 API 安全防护领域取得显著成效。在实际测试与应用场景中，系统成功填补了传统防护技术对 APT 攻击“检测难、响应慢”的空白，将 APT 攻击平均识别时间从传统规则匹配的小时级缩短至毫秒级，问题处置效率提升超 90%；同时，依托多源流量融合与动态联动响应功能，为金融、政务等领域提供了“精准识别－自动处置－态势可视”的一体化防护服务。系统的深度学习模型与闭环防御机制，不仅让 API 安全防护流程更顺畅，还大幅降低了安全事件对业务的干扰，关键业务 API 服务可用性提升至 99.9%以上，防护效果与用户(运维团队)体验均实现显著优化。

本文所提系统的实现采用容器化部署与微服务架构，兼具技术成熟度高、运行稳定性强的特点，核心功能(攻击检测、动态响应、可视化监控)运行可靠，能为关键行业 API 层安全防护提供有力支撑。随着研究与应用的深入，团队也发现当前系统存在一定优化空间：一是对新型未知 APT 攻击的零样本检测能力有待加强，二是跨平台多场景适配的灵活性需进一步提升。基于此，后续将重点开展两方面升级规划：一方面引入联邦学习技术，在保护数据隐私的前提下实现多机构攻击样本共享与模型联合训练；另一方面优化架构设计，增强对边缘计算场景下轻量级 API 的防护适配能力。通过持续的技术迭代与创新，我们相信该系统将在网络安全防护领域发挥更大价值，为数字经济时代的关键信息基础设施安全提供更坚实的保障。

致　谢

衷心感谢参与本项目的各位团队成员的辛勤努力和付出。他们的专业知识和团队协作精神为项目的

顺利进行和取得成功的研究成果做出了重要贡献。

基金项目

本文受哈尔滨师范大学大学生创新创业项目“面向 APT 攻击的智能检测与主动防御系统设计”资助。

参考文献

[1] 李博宇. 基于深度学习的主机异常行为检测技术研究[D]: [硕士学位论文]. 北京: 军事科学院, 2023.

[2] 王燕雯. 基于 CNN-LSTM 算法的恶意软件攻击检测研究[D]: [硕士学位论文]. 天津: 天津财经大学, 2022.

[3] 王帆. 基于深度学习的 APT 攻击流量检测研究[D]: [硕士学位论文]. 郑州: 郑州大学, 2022.

[4] 石梓良, 韦云天. 基于深度学习的网络安全 API 接口异常检测[J]. 计算机产品与流通, 2024(6): 130-132.

[5] 张雨馨. 基于 API 行为特征的恶意代码检测技术研究[D]: [硕士学位论文]. 济南: 齐鲁工业大学, 2024.

[6] 欧绍华. 基于多特征的安卓恶意软件检测方案研究[D]: [硕士学位论文]. 重庆: 重庆邮电大学, 2022.

[7] 刘世一. 基于 API 序列的深度学习恶意软件检测方法的研究与实现[D]: [硕士学位论文]. 北京: 北京邮电大学, 2024.